

# Complementarity and the algebraic structure of 4-level quantum systems

Dénes Petz<sup>1,4,5</sup>, András Szántó<sup>2,5</sup> and Mihály Weiner<sup>3,4</sup>

<sup>4</sup> Alfréd Rényi Institute of Mathematics,  
H-1364 Budapest, POB 127, Hungary

<sup>5</sup> Department for Mathematical Analysis, BUTE,  
H-1521 Budapest, POB 91, Hungary

## Abstract

The history of complementary observables and mutual unbiased bases is reviewed. A characterization is given in terms of conditional entropy of subalgebras. The concept of complementarity is extended to non-commutative subalgebras. Complementary decompositions of a 4-level quantum system are described and a characterization of the Bell basis is obtained.

2000 *Mathematics Subject Classification*. Primary 47L90, 15A90; Secondary 81Q99, 81R05.

*Key words and phrases*. Complementarity, conditional entropy, mutually unbiased bases, Bell basis, subsystem, quantum information, qubits.

The origin of complementarity is related to the non-commutativity of operators describing observables in quantum mechanics. Although the concept was born together with quantum mechanics itself, the rigorous definition was given much later. Complementary bases or complementary measurements give maximal information about the quantum system. Complementarity is used, for example, in state estimation [16, 24] and

---

<sup>1</sup>E-mail: petz@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA T068258.

<sup>2</sup>E-mail: szbandi@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA TS-49835.

<sup>3</sup>E-mail: mweiner@renyi.hu.

in quantum cryptography [2]. When non-classical, say quantum, information is considered, then non-commutative subalgebras or subsystems of the total system should be chosen. The study of complementary non-commutative subalgebras is rather recent [18].

In general, the knowledge of the probability distribution of a single physical quantity is not sufficient for determining the state of a system. On the other hand, a part of the information coming from the distributions of several quantities may be redundant. Intuitively, two quantities are complementary if the knowledge of their distributions is the most informative; i.e. as little redundant as possible.

Maximal precision measurements are related to maximal Abelian subalgebras. However, one is also motivated to study complementarity for non-Abelian subalgebras. For example, units that can be considered in a quantum computer to be qubits are described by subalgebras that are isomorphic to the algebra of  $2 \times 2$  matrices. One might be interested to choose a collection of qubits that are as little redundant as possible. Conditional (or relative) entropy of subalgebras give also some justification of the intuitive meaning of complementarity. We shall show that if the subalgebra  $\mathcal{A}$  is homogeneous and Abelian, then the conditional entropy  $H(\mathcal{A}|\mathcal{B})$  is maximal if and only if  $\mathcal{A}$  and  $\mathcal{B}$  are complementary. It is shown that in general (that is, not assuming  $\mathcal{A}$  to be Abelian) complementarity cannot be characterized by the maximality of the relative entropy. Nevertheless, we shall also discuss in what sense this result supports the intuitive meaning of complementarity in the non-commutative case, too.

The paper contains a detailed analysis the complementary subsystems of two qubits. It is not surprising that the Bell basis can be characterized by complementarity with respect to both qubits. The conditional (or relative) entropy of subalgebras is not really computable, but for maximal Abelian subalgebras the maximum value of the conditional entropy is equivalent to complementarity when the state is tracial. The conditional entropy is estimated very concretely in a particular example.

The content of the paper is arranged in the following way. Section 1 is devoted to some parts of the history of the concept of complementarity. A complete description should be rather hard and would require much more space. Section 2 contains the rigorous definitions in an algebraic setting. In the paper only the finite dimensional situation is discussed. Section 3 is about the relation to the conditional entropy of subalgebras introduced long time ago by Connes and Størmer. The main result says that complementarity is the maximality of the conditional entropy. Section 4 and Section 5 contains the analysis of 4-level quantum systems, or 2 qubits. This is the simplest framework for entanglement and actually maximal entanglement is a kind of complementarity. It is evident that the Bell bases induces a maximal Abelian subalgebra which is complementary to both qubits. It turns out that the converse of this statement is true. Recently a conjecture appeared about the conditional entropy of maximal Abelian subalgebras. In the Appendix we shall show by example that it is false.

# 1 A historical introduction to complementarity

Complementarity appeared in the history of quantum mechanics in the early days of the theory. According to *Wolfgang Pauli*, the new quantum theory could have been called the theory of complementarity [9]. This fact shows the central importance of the notion of **complementarity** in the foundations of quantum mechanics. Unfortunately, the importance did not make clear what the concept really means. The idea of complementarity was in connection with **uncertainty relation** and **measurement** limitations. Wolfgang Pauli wrote to Heisenberg in 1926: “*One may view the world with the  $p$ -eye and one may view it with the  $q$ -eye but if one opens both eyes simultaneously then one gets crazy*”. The distinction between **incompatible** and **complementary** observables was not really discussed. This can be the reason that “complementarity” was avoided in the book [10] of von Neumann, although the mathematical foundations of quantum theory were developed in a generally accepted way. The concept of complementarity was not clarified for many years, but it was accepted that the pair of observables of **position** and **momentum** must be a typical and important example (when complementarity means a relation of observables).

The canonically conjugate position and momentum,  $Q$  and  $P$ , are basic observables satisfying the **commutation relation**,

$$(QP - PQ)f = if \quad (f \in \mathcal{D})$$

which holds on a dense domain  $\mathcal{D}$  (for example, on the Schwartz functions in  $L^2(\mathbb{R})$ ). The **uncertainty relation**,

$$\Delta(Q, f) \Delta(P, f) \geq \frac{1}{2} \quad (f \in \mathcal{D})$$

holds on the same domain. (Recall that  $\Delta(A, f) = \sqrt{\langle f, A^2 f \rangle - \langle f, A f \rangle^2}$  is the variance of the observable  $A$  in the vector state  $f$ .)

The **Fourier connection**  $P = \mathcal{F}^{-1}Q\mathcal{F}$  extends also to the spectral measures  $E^P(\cdot)$  and  $E^Q(\cdot)$ , so that one has

$$E^P(H) = \mathcal{F}^{-1}E^Q(H)\mathcal{F}$$

for all Borel sets  $H \subset \mathbb{R}$ . From the Fourier relation one can deduce that  $E^Q(H_1)f = f$  and  $E^P(H_2)f = f$  for some vector  $f$  and bounded sets  $H_1, H_2 \subset \mathbb{R}$  may hold only in the trivial case  $f = 0$ . Therefore, the following well-known relations for the spectral projections are obtained:

$$E^Q(H_1) \wedge E^P(H_2) = E^Q(H_1) \wedge E^P(\mathbb{R} \setminus H_2) = E^Q(\mathbb{R} \setminus H_1) \wedge E^P(H_2) = 0$$

for all bounded  $H_1, H_2 \subset \mathbb{R}$ , where  $\wedge$  denotes the greatest lower bound in the lattice of projections. For some people, these relations show the **complementarity** of  $Q$  and  $P$ . (It may be of interest to note that  $E^Q(\mathbb{R} \setminus H_1) \wedge E^P(\mathbb{R} \setminus H_2) \neq 0$ , for all bounded

$H_1$  and  $H_2$  [7].)  $Q$  and  $P$  are **totally non-commutative**: There are no vectors with respect to which  $Q$  and  $P$  commute. People have agreed that position and momentum are complementary observables. This opinion was supported by the fact that two observables cannot be measured or tested together [3].

If the Hilbert space of the quantum system is finite dimensional, then the total non-commutativity of two observables is typical. If complementarity means maximal incompatibility, then the definition must be different.

*Herman Weyl* used the finite Fourier transform to approximate the relation of  $P$  and  $Q$  in finite dimensional Hilbert spaces [25]. Let  $|0\rangle, |1\rangle, \dots, |n-1\rangle$  be an orthonormal basis in an  $n$ -dimensional Hilbert space. The transformation

$$V_n : |i\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \omega^{ij} |j\rangle \quad (\omega = e^{2\pi i/n}) \quad (1)$$

is a unitary and it is nowadays called **quantum Fourier transform**. If the operator  $A = \sum_i \lambda_i |e_i\rangle\langle e_i|$  is diagonal in the given basis and  $B = V_n^* A V_n$ , then the pair  $(A, B)$  approximates  $(Q, P)$  when the eigenvalues are chosen properly.

The complementarity of observables of a finite quantum system was emphasized by Accardi in 1983 during the Villa Mondragone conference [1]. His approach is based on conditional probabilities. If an observable is measured on a copy of a quantum system and another observable is measured on another copy (prepared in the same state), then one measurement does not help to guess the outcome of the other measurement, if all conditional probabilities are the same. If the eigenvectors of the first observable are  $\xi_i$ 's, the eigenvectors of the second one are  $\eta_j$ 's and the dimension of the Hilbert space is  $n$ , then complementarity means

$$|\langle \xi_i, \eta_j \rangle| = \frac{1}{\sqrt{n}}. \quad (2)$$

It is clear that the complementarity of two observables is actually the property of the two eigenbases, so it is better to speak about complementary bases. The Fourier transform (1) moves the standard basis  $|0\rangle, |1\rangle, \dots, |n-1\rangle$  to a complementary basis  $V_n|0\rangle, V_n|1\rangle, \dots, V_n|n-1\rangle$ . The complementarity (2) is often called **value complementarity** and it was an important subject in the work of Schwinger [21, 22].

In connection with complementarity, Kraus made a conjecture about the entropy of two observables [6] which was proved by Maasen and Uffink [8].

The goal of state determination is to recover the state of a quantum system by measurements. If the Hilbert space is  $n$  dimensional, then the density matrix of a state contains  $n^2 - 1$  real parameters. If a measurement is repeated on many copies of the same system, then  $n - 1$  parameters can be estimated. Therefore, at least  $n + 1$  different measurement should be performed to estimate the  $n^2 - 1$  parameters. A measurement can be identified with a basis. Wootters and Fields argued that in the optimal situation estimation scheme the  $n + 1$  bases must be pairwise complementary [24]. Instead

of pairwise complementary bases, Wootters and Fields used the expression “**mutually unbiased bases**” and this terminology has become popular. A different kind of optimality of the complementary bases was obtained in [17] in terms of the determinant of the average mean quadratic error matrix.

While Kraus was interested in the number of non-unitarily equivalent complementary pairs, after publication of the paper of Wootters and Fields, the maximum number of mutually unbiased bases become a research subject. (It is still not known if for any dimension  $n$  the upper bound  $n + 1$  is accessible, [23].)

## 2 Complementary subalgebras

Let  $\mathcal{H}$  be an  $n$ -dimensional Hilbert space with an orthonormal basis  $e_1, e_2, \dots, e_n$ . A unit vector  $\xi \in \mathcal{H}$  is **complementary** with respect to the given basis  $e_1, e_2, \dots, e_n$  if

$$|\langle \xi, e_i \rangle| = \frac{1}{\sqrt{n}} \quad (1 \leq i \leq n). \quad (3)$$

When the Hilbert space  $\mathcal{H}$  is a tensor product  $\mathcal{H}_1 \otimes \mathcal{H}_2$ , then a unit vector complementary to a product basis is called **maximally entangled state**. (If a vector is complementary to a product basis, then it is complementary to any other product basis.) When  $\dim \mathcal{H}_1 = \dim \mathcal{H}_2 = 2$ , then the **Bell basis** consists of maximally entangled states.

(3) is equivalent to the formulation that the vector state  $|\xi\rangle\langle\xi|$  gives the uniform distribution when the measurement  $|e_1\rangle\langle e_1|, \dots, |e_n\rangle\langle e_n|$  is performed:

$$\text{Tr } |\xi\rangle\langle\xi| |e_i\rangle\langle e_i| = \frac{1}{n} \quad (1 \leq i \leq n).$$

The unital subalgebra generated by  $|\xi\rangle\langle\xi|$  consists of operators  $\lambda|\xi\rangle\langle\xi| + \mu|\xi\rangle\langle\xi|^\perp$  ( $\lambda, \mu \in \mathbb{C}$ ), while the algebra generated by the orthogonal projections  $|e_i\rangle\langle e_i|$  is  $\{\sum_i \lambda_i |e_i\rangle\langle e_i| : \lambda_i \in \mathbb{C}\}$ . Relation (3) can be reformulated in terms of these generated subalgebras.

**Theorem 1** *Let  $\mathcal{A}_1$  and  $\mathcal{A}_2$  be subalgebras of  $M_k(\mathbb{C})$  and let  $\tau := \text{Tr}/k$  be the normalized trace. Then the following conditions are equivalent:*

- (i) *If  $P \in \mathcal{A}_1$  and  $Q \in \mathcal{A}_2$  are minimal projections, then  $\tau(PQ) = \tau(P)\tau(Q)$ .*
- (ii) *The subalgebras  $\mathcal{A}_1$  and  $\mathcal{A}_2$  are quasi-orthogonal in  $M_n(\mathbb{C})$ , that is the subspaces  $\mathcal{A}_1 \ominus \mathbb{C}I$  and  $\mathcal{A}_2 \ominus \mathbb{C}I$  are orthogonal.*
- (iii)  *$\tau(A_1 A_2) = \tau(A_1)\tau(A_2)$  if  $A_1 \in \mathcal{A}_1$ ,  $A_2 \in \mathcal{A}_2$ .*
- (iv) *If  $E_1 : \mathcal{A} \rightarrow \mathcal{A}_1$  is the trace preserving conditional expectation, then  $E_1$  restricted to  $\mathcal{A}_2$  is a linear functional (times  $I$ ).*

This theorem was formulated in [18] and led to the concept of complementary subalgebras. Namely  $\mathcal{A}_1$  and  $\mathcal{A}_2$  are complementary if the conditions of the theorem hold. As we explained above complementary maximal Abelian subalgebras is a popular subject in the form of the corresponding bases. We note that complementary MASA's was studied also in von Neumann algebras [20]

Two orthonormal bases are connected by a unitary. It is quite obvious that two bases are mutually unbiased if and only if the absolute value of the elements of the transforming unitary is the same,  $1/\sqrt{n}$  when  $n$  is the dimension. This implies that construction of mutually unbiased bases is strongly related (or equivalent) to the search for Hadamard matrices.

Let  $\mathcal{A}_1$  and  $\mathcal{A}_2$  be subalgebras of  $M_k(\mathbb{C})$  and assume that both subalgebras are isomorphic to  $M_m(\mathbb{C})$ . Then  $k = mn$  and we can assume that  $\mathcal{A}_1 = \mathbb{C}I_n \otimes M_m(\mathbb{C})$ . There exists a unitary  $W$  such that  $W\mathcal{A}_1W^* = \mathcal{A}_2$ . The next theorem characterizes  $W$  when  $\mathcal{A}_1$  and  $\mathcal{A}_2$  are complementary [13, 18]. (On the matrices the Hilbert-Schmidt inner product  $\langle A, B \rangle = \text{Tr } A^*B$  is considered.)

**Theorem 2** *Let  $E_i$  be an orthonormal basis in  $M_n(\mathbb{C})$  and let  $W = \sum_i E_i \otimes W_i \in M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$  be a unitary. The subalgebra  $W(\mathbb{C}I_n \otimes M_m(\mathbb{C}))W^*$  is complementary to  $\mathbb{C}I \otimes M_m(\mathbb{C})$  if and only if*

$$\frac{m}{n} \sum_k |W_k\rangle\langle W_k|$$

*is the identity mapping on  $M_m(\mathbb{C})$ .*

The condition in the Theorem cannot hold if  $m < n$  and in the case  $n = m$  the condition means that  $\{W_k : 1 \leq k \leq n^2\}$  is an orthonormal basis in  $M_m(\mathbb{C})$ .

A different method for the construction of complementary subalgebras is indicated in the next example.

**Example 1** Assume that  $p > 2$  is prime. Let  $e_0, e_1, \dots, e_{p-1}$  be a basis and let  $X$  be the unitary operator permuting the basis vectors cyclically:

$$Xe_i = \begin{cases} e_{i+1} & \text{if } 0 \leq i \leq p-2, \\ e_0 & \text{if } i = p-1. \end{cases}$$

Let  $q := e^{i2\pi/p}$  and define another unitary by  $Ze_i = q^i e_i$ . Their matrices are as follows.

$$X = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & q & 0 & \cdots & 0 \\ 0 & 0 & q^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & q^{p-1} \end{bmatrix}.$$

It is easy to check that  $ZX = qXZ$  or more generally the relation

$$(X^{k_1} Z^{\ell_1})(X^{k_2} Z^{\ell_2}) = q^{k_2 \ell_1} X^{k_1+k_2} Z^{\ell_1+\ell_2}. \quad (4)$$

is satisfied. The unitaries

$$\{X^j Z^k : 0 \leq j, k \leq p-1\}$$

are pairwise orthogonal.

For  $0 \leq k_1, \ell_1, k_2, \ell_2 \leq p-1$  set

$$\pi(k_1, \ell_1, k_2, \ell_2) = X^{k_1} Z^{\ell_1} \otimes X^{k_2} Z^{\ell_2}.$$

From (4) we can compute

$$\pi(u)\pi(u') = q^{-u \circ u'} \pi(u')\pi(u), \quad (5)$$

where

$$u \circ u' = k_1 \ell'_1 - k'_1 \ell_1 + k_2 \ell'_2 - k'_2 \ell_2 \pmod{p}$$

for  $u = (k_1, \ell_1, k_2, \ell_2)$  and  $u' = (k'_1, \ell'_1, k'_2, \ell'_2)$ . Hence  $\pi(u)$  and  $\pi(u')$  commute if and only if  $u \circ u'$  equals zero.

We want to define a homomorphism  $\rho : M_p(\mathbb{C}) \rightarrow M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$  such that

$$\rho(X) = \pi(k_1, \ell_1, k_2, \ell_2) \quad \text{and} \quad \rho(Z^{u \circ u'}) = \pi(u')$$

when  $u \circ u' \neq 0$ . Since the commutation relation (5) is the same as that for  $X$  and  $Z^{u \circ u'}$ ,  $\rho$  can be extended to an embedding of  $M_p(\mathbb{C})$  into  $M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$ . Let  $\mathcal{A}(u, u') \subset M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$  be the range. This is a method to construct subalgebras. For example, if

$$\pi(u) = X \otimes X \quad \text{and} \quad \pi(u') = Z \otimes Z,$$

then the generated subalgebra  $\mathcal{A}(u, u')$  is obviously complementary to  $\mathbb{C}I \otimes M_p(\mathbb{C})$  and  $M_p(\mathbb{C}) \otimes \mathbb{C}I$ . (At this point we used the condition  $p > 2$ , since this implies that  $X$  and  $Z$  do not commute.)  $\square$

The idea of the above example is used by Ohno to construct  $p^2 + 1$  complementary subalgebras in  $M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$  [12].

### 3 Conditional entropy

Let  $\mathcal{A}$  and  $\mathcal{B}$  be subalgebras of  $\mathcal{M} \equiv M_n(\mathbb{C})$ . For a state  $\psi$  on  $\mathcal{M}$  the **conditional entropy** of the algebras  $\mathcal{A}$  and  $\mathcal{B}$  is defined as

$$H_\psi(\mathcal{A}|\mathcal{B}) := \sup \left\{ \sum_i \lambda_i \left( S(\psi_i|_{\mathcal{A}} \| \psi|_{\mathcal{A}}) - S(\psi_i|_{\mathcal{B}} \| \psi|_{\mathcal{B}}) \right) \right\} \quad (6)$$

where the supremum is taken over all possible decomposition of  $\psi$  into a convex combination  $\psi = \sum_i \lambda_i \psi_i$  of states and  $S(\cdot \| \cdot)$  stands for the relative entropy of states.

This concept was introduced by Connes and Størmer in 1975 [5] and was called relative entropy of subalgebras. Since in the case of commutative algebras, the quantity becomes the usual conditional entropy, see Chap. 10 in [11], we are convinced that conditional entropy is the proper terminology.

If  $\mathcal{B} = \mathbb{C}I$ , then  $H_\psi(\mathcal{A}|\mathcal{B})$  is the entropy

$$H_\psi(\mathcal{A}) = \sup \left\{ \sum_i \lambda_i \left( S(\psi_i|_{\mathcal{A}} \| \psi|_{\mathcal{A}}) \right) \right\}$$

of the subalgebra  $\mathcal{A}$  [14]. The quantity  $H_\psi(\mathcal{A})$  is heuristically the amount of information contained in the subalgebra  $\mathcal{A}$  about the state. In this spirit, the conditional entropy measures the information difference carried by  $\mathcal{A}$  and  $\mathcal{B}$  together with respect to  $\mathcal{B}$ . Formally we can state much less. For example,  $H_\psi(\mathcal{A}|\mathcal{B}) = 0$  if and only if  $\mathcal{A} \subset \mathcal{B}$  [11]. We have  $H_\psi(\mathcal{A}|\mathcal{B}) \leq H_\psi(\mathcal{A})$  and in probability theory the equality is equivalent to the independence of  $\mathcal{A}$  and  $\mathcal{B}$  (with respect to  $\psi$ ). Here we are interested in the tracial state in the role of  $\psi$  and want to study the relation of the maximality of the conditional entropy to the complementarity of the subalgebras.

One may wonder whether at taking supremum, we should really consider all possible decompositions. Indeed, from the point of view of actual calculations, it is a rather unfortunate thing, as in some sense they are “too many” to parametrize.

**Lemma 1** *It is enough to take the supremum in (6) over all possible decomposition of  $\psi$  into a convex combination  $\psi = \sum_i \lambda_i \psi_i$  of linearly independent states (over  $\mathbb{R}$ ).*

*Proof:* Let  $\psi = \sum_{i=1}^k \lambda_i \psi_i$  be a decomposition of  $\psi$  into a convex combination of states. Without the loss of generality, we may assume that all  $\lambda_i$  weights are nonzero. (States with zero weights can be simply left out both from the decomposition and from the expression of the entropy, too.) Suppose there is a nontrivial real-linear dependence between the states appearing in the decomposition; that is, we have that  $\sum_{i=1}^k \alpha_i \psi_i = 0$  for a collection of nontrivial real coefficients  $\alpha_i$ . Then with

$$\lambda_i(t) := \lambda_i + \alpha_i t, \quad \text{we have} \quad \psi = \sum_{i=1}^k \lambda_i(t) \psi_i.$$

Since  $\min\{\lambda_i\} > 0$ , there is an interval  $I \subset \mathbb{R}$  having 0 as an interior point, such that  $\lambda_i|_I \geq 0$  for all indices. In fact, it is rather evident, that there exists a maximal such interval, say  $I_{\max}$ , and that  $I_{\max} = [a, b]$  is closed and there exist some indices  $j_a$  and  $j_b$  such that at the endpoints of the interval  $\lambda_{j_a}(a) = \lambda_{j_b}(b) = 0$ . Since the function  $h$  defined by the formula

$$h(t) := \sum_i \lambda_i(t) \left( S(\psi_i|_{\mathcal{A}} \| \psi_i|_{\mathcal{A}}) - S(\psi_i|_{\mathcal{B}} \| \psi|_{\mathcal{B}}) \right)$$

is a polynomial of order at most one, we have that  $h(0) \leq \max\{h(a), h(b)\}$ . In other words, we may change the original sum (i.e. the sum at parameter  $t = 0$ ) by letting



$t = a$  or  $t = b$  in such a way, that its value will not decrease. However, the sum at parameter  $t = a$  ( $t = b$ ) corresponds to a convex combination of the states  $\psi_i$  with  $i \neq j_a$  ( $i \neq j_b$ ). In other words, using the linear dependence we can eliminate at least one of the states appearing in the decomposition in such a way that the sum will surely not decrease. This verifies our claim since we may repeat this process until the set of states in question will be linearly independent.  $\square$

It is a consequence of the lemma that in the finite dimensional case, the word “supremum” appearing in the definition of conditional entropy can be replaced by the word “maximum”. (A standard argument relies on the continuity of the entropy functional and the compactness of the state space.)

In what follows the reference state  $\psi$  will be always the unique normalized tracial state  $\tau := \text{Tr} / n$  on  $\mathcal{M} \equiv M_n(\mathbb{C})$ . So we shall omit the indication of the reference state and simply write  $H(\mathcal{A}|\mathcal{B})$  instead of  $H_\tau(\mathcal{A}|\mathcal{B})$ . Also, instead of the states  $\psi_i$ , it will be often convenient to work with their density matrices  $\rho_i$  with respect to  $\tau$ . It is an easy exercise to check that the conditional entropy is expressed with density matrices as

$$H(\mathcal{A}|\mathcal{B}) = \sup \left\{ \sum_i \lambda_i \left( \tau(\eta(E_{\mathcal{B}}\rho_i)) - \tau(\eta(E_{\mathcal{A}}\rho_i)) \right) \right\}, \quad (7)$$

where  $E_{\mathcal{A}} : \mathcal{M} \rightarrow \mathcal{A}$  and  $E_{\mathcal{B}} : \mathcal{M} \rightarrow \mathcal{B}$  are the  $\tau$ -preserving conditional expectations,  $\eta(t) = -t \log t$ , and the supremum is taken over all possible convex decompositions of the identity  $I = \sum_i \lambda_i \rho_i$ .

Our primary interest concerns the case when the subalgebras in question are either maximal Abelian or isomorphic to some full matrix algebras. The two cases will be discussed together; for our argument it will be enough to assume that all minimal projections of  $\mathcal{A}$  have the same trace. Such subalgebra  $\mathcal{A}$  will be called **homogeneous**. Suppose that for every minimal projection  $p \in \mathcal{A}$  we have  $\tau(p) = d$ . Then for every density operator  $\rho$  and minimal projection  $p \in \mathcal{A}$ , we have that

$$\tau(\eta(E_{\mathcal{A}}(\rho))) \geq \tau(\eta(p/d)) = \log d,$$

and equality holds if and only if  $dE_{\mathcal{A}}(\rho)$  is a minimal projection of  $\mathcal{A}$ , which is trivially further equivalent with the fact that the range of  $\rho$  is contained in the range of a minimal projection of  $\mathcal{A}$ . On the other hand,

$$\tau(\eta(E_{\mathcal{B}}(\rho))) \leq \tau(\eta(I)) = 0.$$

This implies that

$$H(\mathcal{A}|\mathcal{B}) \leq -\log d. \quad (8)$$

In general it is easy to give some sufficient conditions ensuring that in the above inequality one has equality. When  $\mathcal{A}$  is Abelian, we can also give a simple necessary condition.

**Lemma 2** *Let  $\mathcal{A}$  be a homogeneous subalgebra such that  $\tau(p) = d$  for the minimal projections  $p \in \mathcal{A}$ . If there exists a decomposition  $I = \sum_i \lambda_i p_i$  of the identity such that  $\lambda_i > 0$  and  $p_i$  are minimal projections of  $\mathcal{A}$  satisfying  $E_{\mathcal{B}}(p_i) = dI$ , then equality holds in (8).*

*Proof:* It is enough to give a lower estimate for the conditional entropy:

$$\begin{aligned} H(\mathcal{A}|\mathcal{B}) &\geq \sum_i \lambda_i d \left( \tau(\eta(E_{\mathcal{B}}(p_i/d))) - \tau(\eta(E_{\mathcal{A}}(p_i/d))) \right) \\ &= \sum_i \lambda_i d \left( \tau(\eta(I)) - \tau(\eta(p_i/d)) \right) = \sum_i \lambda_i d \log(1/d) = -\log d, \end{aligned} \quad (9)$$

since from  $1 = \tau(I) = \tau(\sum_i \lambda_i p_i)$  we get that  $\sum_i \lambda_i d = 1$ .  $\square$

**Theorem 3** *Let  $\mathcal{A}$  and  $\mathcal{B}$  be subalgebras of  $M_n(\mathbb{C})$ . Assume that  $\mathcal{A}$  is Abelian and homogeneous. Then the subalgebras  $\mathcal{A}$  and  $\mathcal{B}$  are complementary if and only if  $H(\mathcal{A}|\mathcal{B})$  is maximal.*

*Proof:* If  $\mathcal{A}$  and  $\mathcal{B}$  are complementary, then for the minimal projections  $p_i$  of  $\mathcal{A}$ ,  $\sum_i p_i = I$  and  $E_{\mathcal{B}}(p_i) = dI$  hold. So Lemma 2 tells us that the conditional entropy is  $-\log d$ .

Assume now that  $H(\mathcal{A}|\mathcal{B}) = -\log d$ . Then there exists a decomposition  $I = \sum_i \lambda_i \rho_i$  of the identity into a convex combination of density operators such that  $E_{\mathcal{B}}(\rho_i) = I$  and  $q_i := E_{\mathcal{A}}(\rho_i)/n$  are minimal projections of  $\mathcal{A}$ .

Suppose that the image under the trace-preserving expectation  $E$  onto a subalgebra of a positive operator  $a$  is a multiple of a minimal projection  $p$  of the subalgebra. Then  $x := (I - p)a(I - p)$  is a positive operator for which

$$E(x) = (I - p)E(a)(I - p) = 0,$$

and hence  $x = 0$ . It follows that  $(I - p)\sqrt{a} = 0$  and we conclude  $pa = ap = a$ .

Applying the above, we have that for every minimal projection  $q$  of  $\mathcal{A}$

$$q = qI = q \sum_i \lambda_i \rho_i = q \sum_i \lambda_i q_i \rho_i = \sum_i \lambda_i q q_i \rho_i = \sum_{\{i: q_i = q\}} \lambda_i q_i \rho_i = \sum_{\{i: q_i = q\}} \lambda_i \rho_i,$$

since the product  $qq_i$  is zero, when  $q_i \neq q$  and  $q_i$  when  $q_i = q$ . (Note that this is the point where we have used the fact the  $\mathcal{A}$  is Abelian). As  $E_{\mathcal{B}}(\rho_i) = I$ , the above decomposition of  $q$  shows that  $E_{\mathcal{B}}(q)$  is a multiple of the identity, and hence (as  $q$  was arbitrary, and the minimal projections of  $\mathcal{A}$  span the whole algebra  $\mathcal{A}$ ) that  $\mathcal{A}$  is quasi-orthogonal to  $\mathcal{B}$ .  $\square$

Let  $\mathcal{A}$  and  $\mathcal{B}$  be subalgebras of  $M_n(\mathbb{C})$ . Assume that  $\mathcal{A}$  is Abelian and homogeneous and choose a homogeneous algebra  $\mathcal{C}$  such that  $\mathcal{A}$  is maximal Abelian subalgebra of  $\mathcal{C}$ . If  $\mathcal{A}$  and  $\mathcal{B}$  are complementary, then  $H(\mathcal{C}|\mathcal{B})$  is maximal (that is, equals  $H(\mathcal{C})$ ). However,  $\mathcal{C}$  and  $\mathcal{B}$  is not necessarily complementary, in fact it is fairly easy to come up with an example in which their intersection is not trivial. Hence the conditional entropy cannot characterize the complementarity of subalgebras in the general case.

Suppose we are dealing with two subsystems (that is, subalgebras)  $\mathcal{B}, \mathcal{C}$  of a finite level quantum system (that is,  $M_n(\mathbb{C})$ ). Knowing the restriction of the state to  $\mathcal{B}$  might help

in predicting results of measurements performed on  $\mathcal{C}$ . However, a (maximal precision) measurement on  $\mathcal{C}$  corresponds to a maximal Abelian subalgebra of  $\mathcal{C}$ . Hence the natural interpretation of complementarity suggests that complementarity of  $\mathcal{B}$  and  $\mathcal{C}$  should mean that for *all* maximal Abelian subalgebras  $\mathcal{A}$  of  $\mathcal{C}$  the conditional entropy  $H(\mathcal{A}, \mathcal{B})$  should be maximal. By what was proved in this section, if  $\mathcal{A}$  is homogeneous, then this condition indeed characterizes complementarity.

## 4 4-level quantum systems

A 4-level quantum system is mathematically the Hilbert space  $\mathbb{C}^4$  or the algebra  $\mathcal{M} := M_4(\mathbb{C})$ . We are interested in two kinds of subalgebras.

An **F-subalgebra** is a subalgebra isomorphic to  $M_2(\mathbb{C})$ . “F” is the abbreviation of “factor”, the center of such a subalgebra is minimal,  $\mathbb{C}I$ . If our 4-level quantum system is regarded as two qubits, then an F-subalgebra may correspond to one of the qubits. When the F-subalgebra  $\mathcal{A}_0$  describes a “one-qubit-subsystem”, then the relative commutant  $\mathcal{A}' := \{B \in \mathcal{M} : BA = AB \text{ for every } A \in \mathcal{A}\}$  corresponds to the other qubit. If  $\mathcal{A}$  is an F-subalgebra of  $\mathcal{M}$ , then we may assume that  $\mathcal{M} = \mathcal{A} \otimes \mathcal{A}'$ .

An **M-subalgebra** is a maximal Abelian subalgebra, equivalently, it is isomorphic to  $\mathbb{C}^4$ . (M is an abbreviation of “MASA”, the center is maximal, it is the whole subalgebra.) An M-subalgebra is in relation to a **von Neumann measurement**, its minimal projections give a partition of unity.

Both the F-subalgebras and the M-subalgebras are 4 dimensional. We define a **P-unitary** as a self-adjoint traceless unitary operator. The eigenvalues of a P-unitary from  $\mathcal{M}$  are  $-1, -1, 1, 1$ . An **F-triplet**  $(S_1, S_2, S_3)$  consists of P-unitaries such that  $S_3 = iS_1S_2$ . An **M-triplet**  $(S_1, S_2, S_3)$  consists of P-unitaries such that  $S_3 = S_1S_2$ . One can see that if  $(S_1, S_2, S_3)$  is an X-triplet, then the linear span of  $I, S_1, S_2, S_3$  is an X-subalgebra,  $X=F, M$ .

**Example 2** Consider the unitary  $W = V_{n^2}$  defined in (1) as an  $n \times n$  block-matrix with entries from  $M_n(\mathbb{C})$ . Then the entries form an orthonormal basis in  $M_n(\mathbb{C})$  and Theorem 2 tells us that the Fourier transform can be used to construct a complementary pair.

The Fourier transform sends the standard basis into a complementary one but it can produce non-commutative complementary subalgebras as well. If  $n = 2$ , then we get the following two F-triplets

$$\sigma_0 \otimes \sigma_1, \quad \sigma_0 \otimes \sigma_2, \quad \sigma_0 \otimes \sigma_3$$

and

$$\frac{1}{2}(-\sigma_2 \otimes \sigma_0 - \sigma_2 \otimes \sigma_3 + \sigma_3 \otimes \sigma_0), \frac{1}{2}(-\sigma_2 \otimes \sigma_0 - \sigma_2 \otimes \sigma_3 + \sigma_3 \otimes \sigma_0 + \sigma_3 \otimes \sigma_3), -\sigma_1 \otimes \sigma_0.$$

□

In the Hilbert space  $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$  the standard product basis is  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ . The **Bell basis**

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

consists of maximal entangled vectors and so it is complementary to the standard product basis. The Bell basis has important applications, for example, the teleportation of a state of a qubit. We show in Theorem 4 below that the above complementarity property characterizes the Bell basis. Up to local unitary transformations, the Bell basis is unique.

The operators diagonal in the Bell basis form an M-subalgebra which is generated by the M-triplet

$$(\sigma_1 \otimes \sigma_1, \quad \sigma_2 \otimes \sigma_2, \quad \sigma_3 \otimes \sigma_3). \quad (10)$$

We call this standard **Bell triplet**.

**Theorem 4** *Let  $\mathcal{A}$  be an F-subalgebra of  $\mathcal{M}$ . Assume that  $(X, Y, Z)$  is an M-triplet which is orthogonal to  $\mathcal{A}$  and  $\mathcal{A}'$ . Then there are F-triplets  $(A_1, A_2, A_3) \in \mathcal{A}$  and  $(B_1, B_2, B_3) \in \mathcal{A}'$  such that*

$$X = A_1 B_1, \quad Y = A_2 B_2, \quad Z = A_3 B_3.$$

*Proof:* Take an expansion

$$X = \sum_{i=1}^3 (x_i \cdot \sigma) \otimes \sigma_i,$$

where  $x_i \in \mathbb{R}^3$ . Then

$$\begin{aligned} X^2 &= \sum_{i,j=1}^3 (\langle x_i, x_j \rangle \sigma_0 + i(x_i \times x_j) \cdot \sigma) \otimes \sigma_i \sigma_j = \sum_{i=1}^3 (\langle x_i, x_i \rangle \sigma_0 + i(x_i \times x_i) \cdot \sigma) \otimes \sigma_0 \\ &\quad + \sum_{i < j} (\langle x_i, x_j \rangle \sigma_0 + i(x_i \times x_j) \cdot \sigma) \otimes \sigma_i \sigma_j + \sum_{i > j} (\langle x_i, x_j \rangle \sigma_0 + i(x_i \times x_j) \cdot \sigma) \otimes \sigma_i \sigma_j \\ &= \sum_{i=1}^3 \langle x_i, x_i \rangle \sigma_0 \otimes \sigma_0 + \sum_{i < j} (2i(x_i \times x_j) \cdot \sigma) \otimes \sigma_i \sigma_j. \end{aligned}$$

We conclude that

$$x_i \times x_j = 0$$

when  $i \neq j$ . All the three vectors  $x_i$  cannot be 0, so we may assume that  $x_1 \neq 0$ . Then there are  $\lambda, \mu \in \mathbb{R}$  such that  $x_2 = \lambda x_1$  and  $x_3 = \mu x_1$ . So  $X = (x_1 \cdot \sigma) \otimes (\sigma_1 + \lambda \sigma_2 + \mu \sigma_3)$ . Since  $\sum_{i=1}^3 \langle x_i, x_i \rangle = 1$ , for an appropriate number  $\kappa$ , the matrices  $A_1 := \kappa(x_1 \cdot \sigma) \otimes I$  and  $B_1 := \kappa^{-1} I \otimes (\sigma_1 + \lambda \sigma_2 + \mu \sigma_3)$  are P-unitaries and the relations

$$X = A_1 B_1, \quad A_1 X = X A_1, \quad B_1 X = X B_1$$

hold.

Next we show that  $A_1Y = -YA_1$ . Changing the Pauli matrices by unitary transformation, we may assume that  $A_1 = \sigma_1 \otimes I$  and  $B_1 = I \otimes \sigma_1$ . The commutant of  $X = \sigma_1 \otimes \sigma_1$  is the linear span of the 8 matrices

$$\{I, \sigma_1 \otimes I, I \otimes \sigma_1, \sigma_1 \otimes \sigma_1, \} \cup \{\sigma_i \otimes \sigma_j\}_{i,j=2}^3.$$

Recall that  $Y$  is orthogonal to  $\mathcal{A}$  and  $\mathcal{A}'$ , so it must be the linear combination of the matrices  $\{\sigma_i \otimes \sigma_j\}_{i,j=2}^3$ . All of them anticommute with  $A_1$ , therefore so does  $Y$ . The matrix  $A_1Y$  is the linear combination of the matrices  $\{\sigma_1\sigma_i \otimes \sigma_j\}_{i,j=2}^3$ , which implies  $A_1Y \perp \mathcal{A}'$ .

Since  $A_1Y = -YA_1$ , it follows that  $\{A_1, Y, -iA_1Y\}$  is an F-triplet which generates the F-subalgebra  $\mathcal{A}_1$ . The F-subalgebras  $\mathcal{A}_1$  and  $\mathcal{A}'$  are complementary, hence  $\mathcal{A}'_1$  and  $\mathcal{A}$  are complementary as well. The intersection of  $\mathcal{A}'_1$  and  $\mathcal{A}'$  is different from  $\mathbb{C}I$ [13], therefore it contains a non-trivial projection  $Q$  which must have trace 2. It follows that the intersection contains a P-unitary  $B_2 := I - 2Q$ . So  $B_2$  commutes with  $Y$  and let  $A_2 := B_2Y = YB_2$ . We check that  $B_1$  and  $B_2$  anticommute:

$$B_1B_2 = (A_1X)(YA_2) = A_1YXA_2 = -Y(A_1X)A_2 = -(B_2A_2)B_1A_2 = -B_2B_1,$$

since  $B_1 = A_1X$ ,  $XY = YX$ ,  $A_1Y = -YA_1$ ,  $Y = B_2A_2$ ,  $A_2B_1 = B_1A_2$ . Similarly,  $A_1$  and  $A_2$  anticommute.  $Y = A_2B_2$  is obvious. If  $A_3 = iA_1A_2$  and  $B_3 = iB_1B_2$ , then both  $(A_1, A_2, A_3)$  and  $(B_1, B_2, B_3)$  are F-triplets. Finally,

$$Z = XY = A_1B_1A_2B_2 = A_1A_2B_1B_2 = A_3B_3$$

and the proof is complete.  $\square$

If the operators  $A_i$  and  $B_i$  are identified with  $\sigma_i$  ( $i = 1, 2, 3$ ) in the theorem, then the triplet  $(X, Y, Z)$  can be identified with the standard Bell triplet (10).

**Example 3** Let  $\mathcal{A}$  be the algebra generated by the operators  $a_1, a_1^*, a_2, a_2^*$  satisfying the **canonical anticommutation relations**:

$$\{a_1, a_1^*\} = \{a_2, a_2^*\} = I, \{a_1, a_1\} = \{a_1, a_2\} = \{a_1, a_2^*\} = \{a_2, a_2\} = 0,$$

where  $\{A, B\} := AB + BA$ . Let  $\mathcal{A}_1$  be the subalgebra generated  $a_1$  and  $\mathcal{A}_2$  be the subalgebra generated  $a_2$ . Then  $\mathcal{A}_1$  and  $\mathcal{A}_2$  are complementary. In the usual matrix representation

$$a_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad a_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

therefore

$$\mathcal{A}_1 = \left\{ \begin{bmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{bmatrix} \right\}, \quad \mathcal{A}_2 = \left\{ \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & -b \\ 0 & 0 & -c & d \end{bmatrix} \right\}.$$

The subalgebra  $\mathcal{A}_1$  is generated by the F-triplet

$$(\sigma_1 \otimes \sigma_0, \quad \sigma_2 \otimes \sigma_0, \quad \sigma_3 \otimes \sigma_0),$$

and  $\mathcal{A}_2$  is spanned by the F-triplet

$$(\sigma_3 \otimes \sigma_1, \quad \sigma_3 \otimes \sigma_2, \quad \sigma_0 \otimes \sigma_3).$$

Observe that the standard Bell triplet (10) is complementary to both  $\mathcal{A}_1$  and  $\mathcal{A}_2$ .

The parity automorphism is defined by  $\Theta(a_1) = -a_1$  and  $\Theta(a_2) = -a_2$ . It is induced by the unitary  $\sigma_3 \otimes \sigma_3$ :

$$\Theta(x) = (\sigma_3 \otimes \sigma_3)x(\sigma_3 \otimes \sigma_3)$$

The operators  $\sigma_i \otimes \sigma_j$ ,  $0 \leq i, j \leq 3$  are eigenvectors of the parity automorphism. The fixed point algebra is linearly spanned by

$$\sigma_0 \otimes \sigma_0, \quad \sigma_1 \otimes \sigma_1, \quad \sigma_2 \otimes \sigma_2, \quad \sigma_3 \otimes \sigma_3$$

and

$$\sigma_0 \otimes \sigma_3, \quad \sigma_1 \otimes \sigma_2, \quad \sigma_2 \otimes \sigma_1, \quad \sigma_3 \otimes \sigma_0.$$

The first group linearly spans the M-subalgebra corresponding to the Bell basis. It follows that all Bell states are **even**, that is the parity automorphism  $\Theta$  leaves them invariant.  $\square$

## 5 Complementary decompositions

In this section the complementary decompositions of  $\mathcal{M} \equiv M_4(\mathbb{C})$  into F- and M-subalgebras are studied. It is well-known that decomposition into 5 M-subalgebras is possible. (Recall that this fact is equivalent to the existence of 5 mutually unbiased bases in a 4 dimensional space.)

The traceless dimension  $\underline{\dim} \mathcal{A} := \dim(\mathcal{A} \ominus \mathbb{C}I) = \dim \mathcal{A} - 1$  will be used sometimes.

**Theorem 5** *Let  $\mathcal{A}_0$  be an F-subalgebra of  $\mathcal{M}$ ,  $\mathcal{A}'_0$  be its commutant, and let  $\mathcal{B}$  be a subalgebra complementary to  $\mathcal{A}_0$ .*

- (a) *If  $\mathcal{B}$  is an M-subalgebra, then it is complementary to  $\mathcal{A}'_0$ .*
- (b) *If  $\mathcal{B}$  is an F-subalgebra, then either  $\underline{\dim}(\mathcal{A}'_0 \cap \mathcal{B}) = 1$  or  $\mathcal{A}'_0 = \mathcal{B}$ .*

*Proof:* In case (a), let  $(X, Y, Z)$  the M-triplet generating  $\mathcal{B}$ . We can assume, that  $\mathcal{A}_0 = M_2(\mathbb{C}) \otimes \mathbb{C}I$ .

We can also presume, that  $X, Y, Z \notin \mathcal{A}'$ , or otherwise if  $X = I \otimes A$ , then the commutant of  $X$  is generated by the matrices

$$V \otimes A, V \otimes I \quad (V \in M_2(\mathbb{C}))$$

and because of the complementarity of  $\mathcal{B}$  and  $\mathcal{A}_0$ ,  $Y = V_1 \otimes A$  holds, and so  $Z = XY = V_1 \otimes I \in \mathcal{A}_0$ . This is a contradiction.

We can take the expansion

$$X = \sum_{i=0}^3 (x_i \cdot \sigma) \otimes \sigma_i,$$

and from  $X^2 = I$  we conclude that  $x_i \times x_j = 0$  when  $i \neq j$  and they are different from 0. There is an  $x \in \mathbb{R}^3$  such that

$$X = (x \cdot \sigma) \otimes (\lambda \cdot \sigma) + x_0 \cdot \sigma \otimes I$$

holds, and similarly there are  $y, z, y_0, z_0 \in \mathbb{R}^3$  vectors, such that

$$Y = (y \cdot \sigma) \otimes (\lambda \cdot \sigma) + y_0 \cdot \sigma \otimes I,$$

$$Z = (z \cdot \sigma) \otimes (\gamma \cdot \sigma) + z_0 \cdot \sigma \otimes I.$$

From  $X^2 = I$  we can also conclude, that  $x \perp x_0$ ,  $y \perp y_0$  and  $z \perp z_0$ .

Now,  $Z = XY$  is traceless and self-adjoint, so

$$\begin{aligned} XY &= (x \cdot \sigma)(y \cdot \sigma) \otimes (\mu \cdot \sigma)(\lambda \cdot \sigma) + (x \cdot \sigma)(y_0 \cdot \sigma) \otimes \mu \cdot \sigma \\ &\quad + (x_0 \cdot \sigma)(y \cdot \sigma) \otimes \lambda \cdot \sigma + (x_0 \cdot \sigma)(y_0 \cdot \sigma) \otimes I \\ &= -(x \times y) \cdot \sigma \otimes (\mu \times \lambda) \cdot \sigma + (\langle x, y \rangle \langle \mu, \lambda \rangle + \langle x_0, y_0 \rangle) I \otimes I \\ &\quad + I \otimes (\langle x, y_0 \rangle \mu + \langle x_0, y \rangle \lambda) \cdot \sigma \\ &\quad + i(\langle \mu, \lambda \rangle (x \times y) + (x_0 \times y_0)) \cdot \sigma \otimes I + I \otimes \langle x, y \rangle (\mu \times \lambda) \cdot \sigma \\ &\quad + (x \times y_0) \cdot \sigma \otimes \mu \cdot \sigma + (x_0 \times y) \cdot \sigma \otimes \lambda \cdot \sigma \\ &= -(x \times y) \cdot \sigma \otimes (\mu \times \lambda) \cdot \sigma \\ &= z \cdot \sigma \otimes \gamma \cdot \sigma. \end{aligned}$$

so  $z_0 = 0$ , and

$$\begin{aligned} ZX = Y &= (z \cdot \sigma)(x \cdot \sigma) \otimes (\gamma \cdot \sigma)(\mu \cdot \sigma) + (z \cdot \sigma)(x_0 \cdot \sigma) \otimes I \\ &= -(z \times x) \cdot \sigma \otimes (\gamma \times \mu) \cdot \sigma \\ &\quad + (\langle z, x \rangle \langle \gamma, \mu \rangle + \langle z, x_0 \rangle) I \otimes I \\ &\quad + i((z \times x_0) + \langle \gamma, \mu \rangle (z \times x)) \cdot \sigma \otimes I. \end{aligned}$$

Again,  $Y$  is self-adjoint, so  $y_0 = 0$ , and similarly  $x_0 = 0$ .

(b) follows from [13].  $\square$

Although  $\mathcal{M}$  has 5 pairwise complementary M-subalgebras, it does not have 5 pairwise complementary F-subalgebras [19]. The next theorem describes the possible complementary decompositions.

**Theorem 6** *Let  $\mathcal{A}_k$  ( $0 \leq k \leq 4$ ) be pairwise complementary subalgebras of  $\mathcal{M}$  such that all of them is an F-subalgebra or M-subalgebra. If  $\ell$  is the number of F-subalgebras in the set  $\{\mathcal{A}_k : 0 \leq k \leq 4\}$ , then  $\ell \in \{0, 2, 4\}$ , and all those values are actually possible.*

*Proof:* First we give an example of  $\ell = 0$ . The M-triplet

$$\{\sigma_{12}, \sigma_{23}, \sigma_{31}\}, \{\sigma_{13}, \sigma_{21}, \sigma_{32}\}, \{\sigma_{01}, \sigma_{10}, \sigma_{11}\}, \{\sigma_{02}, \sigma_{20}, \sigma_{22}\}, \{\sigma_{03}, \sigma_{30}, \sigma_{33}\}$$

give the M-subalgebras. (Note that this case is about five mutually unbiased bases.)

$\ell = 1$  is not possible, because if  $\mathcal{A}_0$  is an F-algebra, then  $\{\mathcal{A}_i\}_{i>0}$  are also complementary to  $\mathcal{A}'_0$ , so  $\underline{\dim}(\bigcup_{i>0} \mathcal{A}_i) \leq 9$ , so they cannot be pairwise complementary, and this is a contradiction.

$\ell = 2$  is possible. The F-triplets

$$\{\sigma_{01}, \sigma_{02}, \sigma_{03}\}, \{\sigma_{10}, \sigma_{20}, \sigma_{30}\}$$

and the M-triplets

$$\{\sigma_{11}, \sigma_{22}, \sigma_{33}\}, \{\sigma_{12}, \sigma_{23}, \sigma_{31}\}, \{\sigma_{13}, \sigma_{21}, \sigma_{32}\}$$

determine the subalgebras.

$\ell = 3$  is not possible, because if  $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2$  are F-algebras, then  $\{\mathcal{A}_i\}_{i>2}$  are also complementary to  $\mathcal{A}'_0$  and  $\mathcal{A}'_1$ . It is easy to see, that  $\underline{\dim}(\bigcup_{i<3} \mathcal{A}_i \cup \mathcal{A}'_0 \cup \mathcal{A}'_1) \geq 10$ , so  $\underline{\dim}(\bigcup_{i>2} \mathcal{A}_i) \leq 5$ , and they cannot be pairwise complementary.

$\ell = 4$  is possible. The F-triplets are

$$\{\sigma_{01}, \sigma_{02}, \sigma_{03}\}, \{\sigma_{10}, \sigma_{21}, \sigma_{31}\}, \{\sigma_{20}, \sigma_{12}, \sigma_{32}\}, \{\sigma_{30}, \sigma_{13}, \sigma_{23}\}$$

and the M-triplet  $\{\sigma_{11}, \sigma_{22}, \sigma_{33}\}$  spans the Bell subalgebra. It was proved in [13] that this kind of decomposition is essentially unique, given 4 pairwise complementary F-subalgebras the rest is always an M-subalgebra. It follows that  $\ell = 5$  is not possible.  $\square$

## 6 Discussion and conclusion

The motivation for complementary subalgebras was a certain kind of state tomography for two qubits [16] and a systematic study started in [18]. An M-subalgebra (corresponding to a measurement) may give classical information and a (non-commutative)



F-subalgebra quantum information about the total system. The complementarity of M-subalgebras is characterized by conditional entropy, however the single data of conditional entropy does not give the complementarity of F-subalgebras.

The construction of complementary subalgebras needs much research. For a 4-level quantum system a complete description is given in the paper. There is no F-subalgebra complementary to both qubits and there is essentially one M-subalgebra complementary to both qubits, this corresponds to the Bell basis.

The difference between  $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$  and  $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$  is essential. The dimensional upper bound for the number of complementary subalgebras (isomorphic to  $M_n(\mathbb{C})$ ) is  $n^2 + 1$ . This bound is not reached for  $n = 2$  [19] but it is reached if  $n > 2$  is a prime [12]. Some related conjecture is contained in [13].

## Appendix

Let  $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$  be maximal Abelian subalgebras with minimal projections  $p_1, p_2, \dots, p_n$  and  $q_1, q_2, \dots, q_n$ . It was expected in [4] that

$$H(\mathcal{A}|\mathcal{B}) = \frac{1}{n} \sum_{i,j=1}^n \eta(\text{Tr}(p_i q_j)). \quad (11)$$

We want to analyse the case  $n = 2$  and show that this formula is not true. (Unfortunately, the correction of the formula seems to be a hard problem.)

Let  $\mathcal{A}$  be the algebra of diagonal matrices, the algebra generated by  $\sigma_3$  and let  $\mathcal{B}$  be the algebra generated by  $\sin \beta \sigma_1 + \cos \beta \sigma_3$ . Then the minimal projections are

$$p := \frac{1}{2}(I + \sigma_3) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad q = \frac{1}{2}(I + (\sin \beta) \sigma_1 + (\cos \beta) \sigma_3).$$

Then the right-hand-side of (11) is

$$C := \eta\left(\frac{1 + \cos \beta}{2}\right) + \eta\left(\frac{1 - \cos \beta}{2}\right).$$

Let  $r(t)$  be a parametrized family of minimal projections in  $M_2(\mathbb{C})$ . Then

$$I = \frac{1}{2}(2r(t)) + \frac{1}{2}(2I - 2r(t))$$

can be considered as a convex decomposition of the identity in (7) and we have

$$H(\mathcal{A}|\mathcal{B}) \geq \eta(b(t)) + \eta(1 - b(t)) - \eta(a(t)) - \eta(1 - a(t)) =: f(t)$$

for all  $t \in \mathbb{R}$ , where  $a(t) := \text{Tr}(r(t)p)$  and  $b := \text{Tr}(r(t)q)$ . Choose

$$r(t) := \frac{1}{2}(I + (\sin t) \sigma_1 + (\cos t) \sigma_3).$$

Then  $f(0)$  equals to  $C$ . However, it is a matter of computation to check that  $f$  is differentiable, and that if  $\beta$  is such that neither  $\sin \beta \neq 0$ , nor  $\cos \beta \neq 0$ , then  $f'(0) \neq 0$ . Thus in general  $f$  cannot have a maximum at  $t = 0$ , and hence (11) is not true.

## References

- [1] L. Accardi, Some trends and problems in quantum probability, in *Quantum probability and applications to the quantum theory of irreversible processes*, eds. L. Accardi, A. Frigerio and V. Gorini, Lecture Notes in Math. **1055**, 1–19. Springer, 1984.
- [2] D. Bruss, Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, **81**, 3018–3021, 1998.
- [3] P. Busch and P.J. Lahti, The complementarity of quantum observables: theory and experiment, *Riv. Nuovo Cimento* **18**(1995), 27 pp.
- [4] M. Choda, lecture at the workshop “*Non-commutative harmonic analysis with applications to probability*”, Bedlewo, 2007.
- [5] A. Connes and E. Størmer, Entropy of  $II_1$  von Neumann algebras, *Acta Math.* **134**(1975), 289–3006.
- [6] K. Kraus, Complementary observables and uncertainty relations. *Phys. Rev. D* (3) **35**(1987), 3070–3075.
- [7] A. Lenard, The numerical range of a pair of projections, *J. Funct. Anal.* **10** (1972) 410–423.
- [8] H. Maassen and I. Uffink, Generalized entropic uncertainty relations, *Phys. Rev. Lett.* **60**(1988), 1103–1106.
- [9] W. Pauli, *General Principles of Quantum Mechanics*, Springer, Berlin, 1980 (original German edition: 1933).
- [10] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, Berlin, 1981. (Original edition: 1932).
- [11] S. Neshveyev and E. Størmer, *Dynamical entropy in operator algebras*, Springer-Verlag, Berlin, 2006.
- [12] H. Ohno, Quasi-orthogonal subalgebras of matrix algebras, preprint, arXiv:0801.1353, 2008.
- [13] H. Ohno, D. Petz and A. Szántó, Quasi-orthogonal subalgebras of  $4 \times 4$  matrices, *Linear Alg. Appl.* **425**(2007), 109–118.

- [14] M. Ohya and D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag, Heidelberg, 1993. Second edition 2004.
- [15] J. Oppenheim, K. Horodecki, M. Horodecki, P. Horodecki and R. Horodecki, A new type of complementarity between quantum and classical information, *Phys. Rev. A* **68**, 022307, 2003.
- [16] D. Petz, K.M. Hangos, A. Szántó and F. Szöllősi, State tomography for two qubits using reduced densities, *J. Phys. A*, **39**, 10901–10907, 2006.
- [17] D. Petz, K.M. Hangos and A. Magyar, Point estimation of states of finite quantum systems, *J. Phys. A*, **40**(2007), 7955–7969.
- [18] D. Petz, Complementarity in quantum systems, *Rep. Math. Phys.* **59**(2007), 209–224.
- [19] D. Petz and J. Kahn, Complementary reductions for two qubits, *J. Math. Phys.*, **48**(2007), 012107.
- [20] S. Popa, Orthogonal pairs of  $*$ -subalgebras in finite von Neumann algebras, *J. Operator Theory* **9**(1983), 253–268.
- [21] M. Rédei, *Quantum Logic in Algebraic Approach*, Fundamental Theories of Physics Vol. **91**, Kluwer Academic Publishers, Dordrecht, Boston and London, 1998.
- [22] J. Schwinger, Unitary operator bases, *Proc. Nat. Acad. Sci. U.S.A.* **46**, 570–579, 1960.
- [23] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13**(2006), 133–177.
- [24] W.K. Wootters and B.D. Fields, Optimal state determination by mutually unbiased measurements, *Ann. Physics*, **191**, 363–381, 1989.
- [25] H. Weyl, *Theory of groups and quantum mechanics*, Methuen, 1931. (Reprint: Dover, 1950)